Defending the United States in the Digital Age

The Importance of Enterprise Architecture and Software Assurance

September 28, 2010

Dr. Ron Ross

Computer Security Division

Information Technology Laboratory

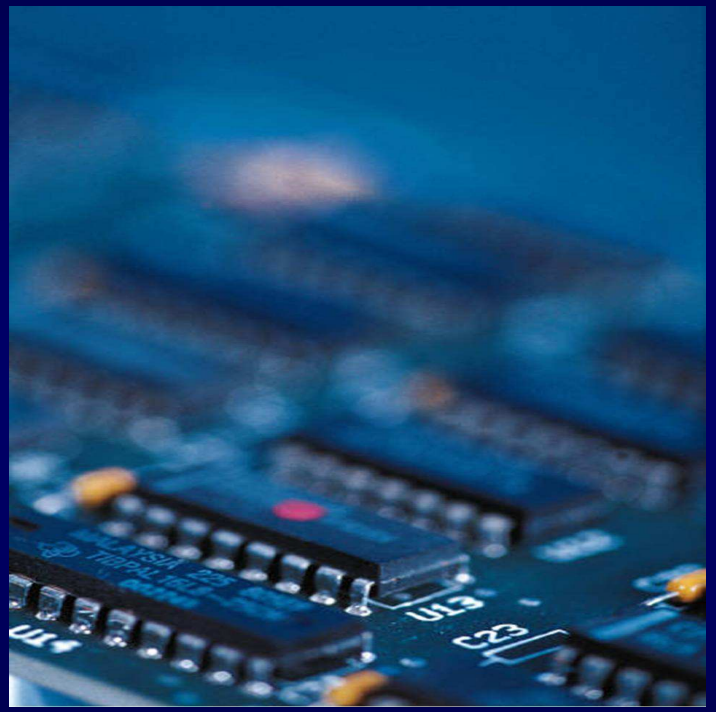
The Stuxnet Worm

Targeting critical infrastructure companies—

- Infected industrial control systems around the world.
- Uploads payload to Programmable Logic Controllers.
- Gives attacker control of the physical system.
- Provides back door to steal data and remotely and secretly control critical plant operations.
- Found in Siemens Simatic Win CC software used to control industrial manufacturing and utilities.

Unconventional Threats to Security

Connectivity



Complexity

Trustworthy Information Systems

- Trustworthy information systems are systems that are worthy of being trusted to operate within defined levels of *risk* to organizational operations and assets, individuals, other organizations, or the Nation despite:
  - ***environmental disruptions***
  - ***human errors***
  - ***purposeful attacks***

  that are expected to occur in the specified environments of operation.

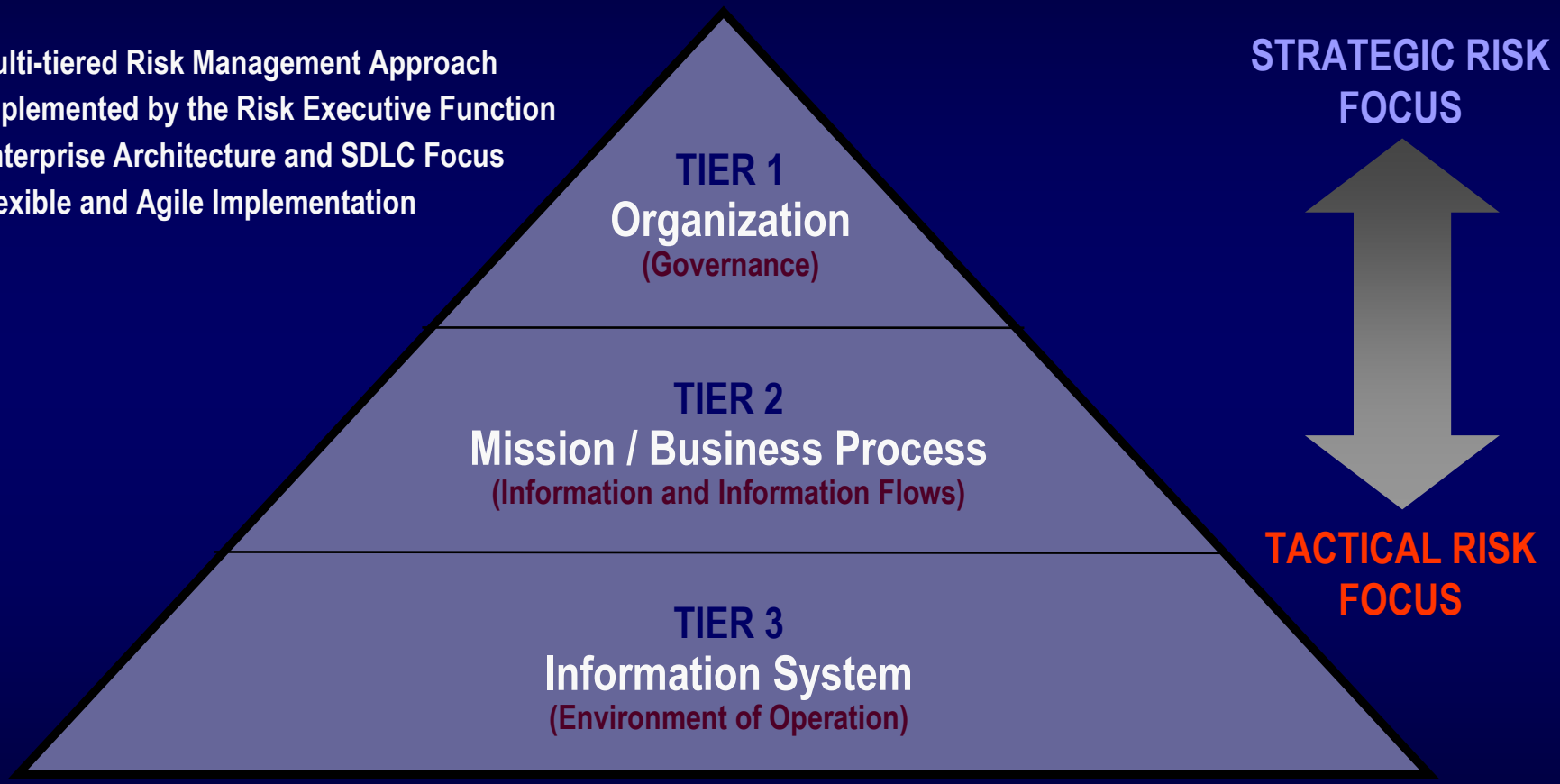
Information System Trustworthiness

Two factors affecting the trustworthiness of information systems include:

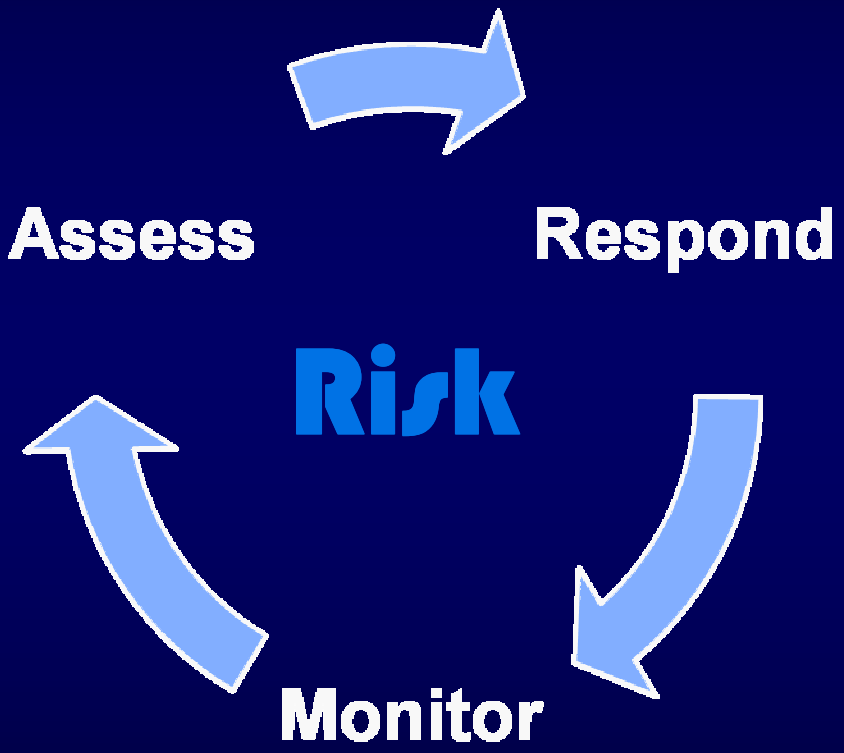
- ***Security functionality*** (i.e., the security-related features or functions employed within an information system or the infrastructure supporting the system); and
- ***Security assurance*** (i.e., the grounds for confidence that the security functionality, when employed within an information system or its supporting infrastructure, is effective in its application).

Enterprise-Wide Risk Management

- Multi-tiered Risk Management Approach
- Implemented by the Risk Executive Function
- Enterprise Architecture and SDLC Focus
- Flexible and Agile Implementation



Risk Management Process



How do we deal with the advanced persistent threat?

The Central Question

From Two Perspectives

- **Security Capability Perspective**
  What security capability is needed to defend against a specific class of cyber threat, avoid adverse impacts, and achieve mission success? **(REQUIREMENTS DEFINITION)**
- **Threat Capability Perspective**
  Given a certain level of security capability, what class of cyber threat can be addressed and is that capability sufficient to avoid adverse impacts and achieve mission success? **(GAP ANALYSIS)**

Cyber Preparedness

An increasingly sophisticated and motivated threat requires increasing preparedness…

Dual Protection Strategies

- **Boundary Protection**

  Primary Consideration: ***Penetration Resistance***
  Adversary Location: ***Outside the Defensive Perimeter***
  Objective: ***Repelling the Attack***

- **Agile Defense**

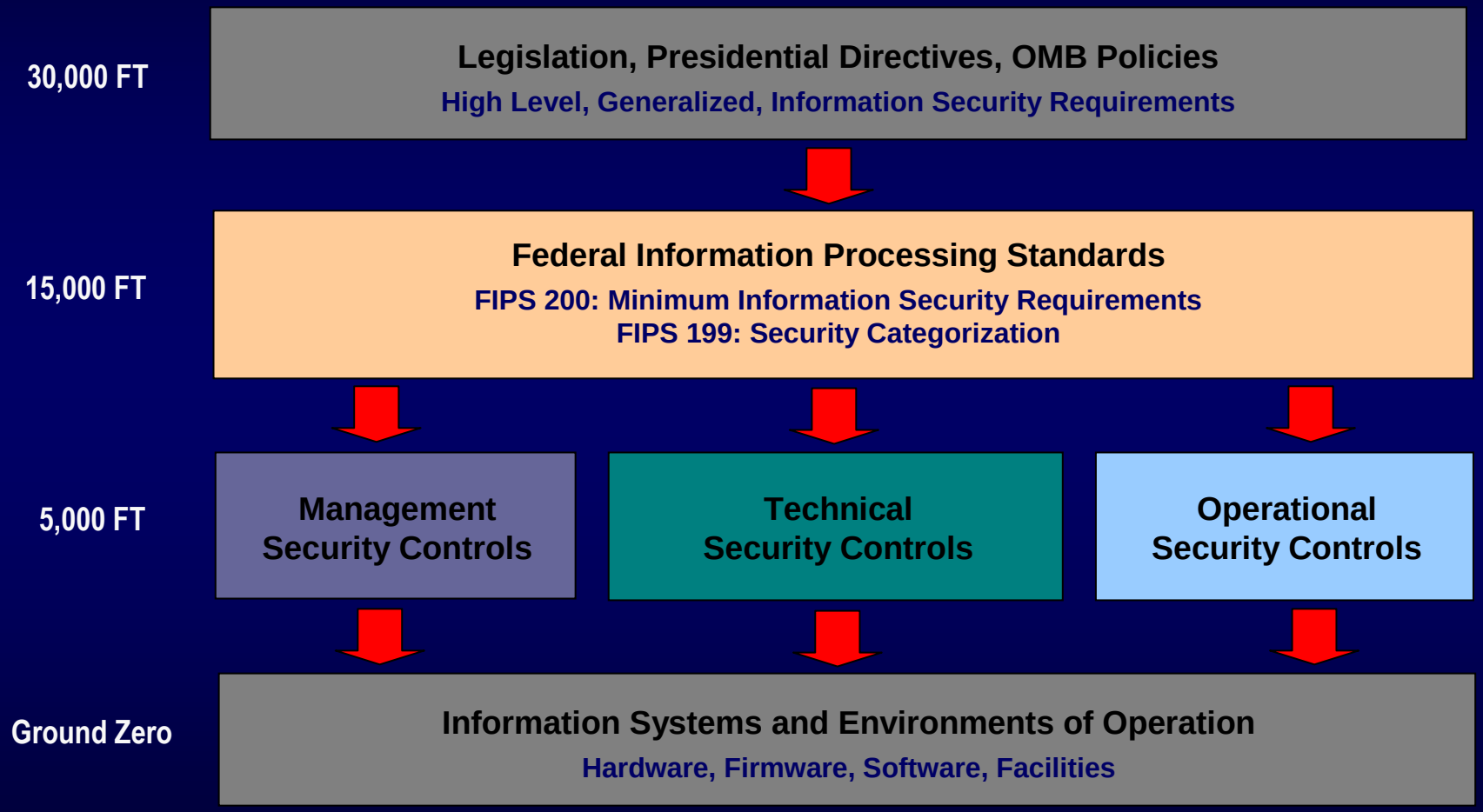
  Primary Consideration: ***Information System Resilience***
  Adversary Location: ***Inside the Defensive Perimeter***
  Objective: ***Operating while under Attack***

Agile Defense

- Boundary protection is a necessary but not sufficient condition for *Agile Defense*
- Examples of *Agile Defense* measures:
  - Compartmentalization and segregation of critical assets
  - Targeted allocation of security controls
  - Virtualization and obfuscation techniques
  - Encryption of data at rest
  - Limiting of privileges
  - Routine reconstitution to known secure state

Bottom Line: Limit damage of hostile attack while operating in a (potentially) degraded mode…

Security Requirements Traceability



Security Control Families

Supporting Software Assurance

- Program Management
  - Mission/Business Process Definition
  - Enterprise Architecture
  - Risk Management Strategy
  - Information Security Resources
  - Information Security Measures of Performance
- System and Services Acquisition
  - Resource Allocation
  - Acquisition and Life Cycle Support
  - Security Engineering Principles
  - Developer Configuration Management and Testing
  - Trustworthiness and Critical Information System Components
  - Supply Chain

Security Control Families

Supporting Software Assurance

- Configuration Management
  - Configuration Change Control
  - Security Impact Analysis
  - Access Restrictions for Change
  - Configuration Settings
  - Least Functionality
- System and Information Integrity
  - Security Functionality Verification
  - Software and Information Integrity
  - Information Input Validation
  - Error Handling
  - Predictable Failure Prevention

Security Control Families

Supporting Software Assurance

- System and Communications Protection
  - Application Partitioning
  - Security Function Isolation
  - Information Shared Resources
  - Trusted Path
  - Transmission of Security Attributes
  - Fail in Known State
  - Thin Nodes

Assurance Requirements

ISO/IEC 15408

- Developer actions.
- Content and presentation of evidence.
- Evaluator actions.

Assurance Requirements

Special Publication 800-53

- The security control is in effect and meets explicitly identified functional requirements in the control statement.
- The control developer/implementer provides a description of the functional properties and design/implementation of the control with sufficient detail to permit analysis and testing of the control.

Assurance Requirements

Special Publication 800-53

- The control developer/implementer includes as an integral part of the control, actions supporting increased confidence that when the control is implemented, it will continuously and consistently meet its required function or purpose and support improvement in the effectiveness of the control.
- The control is developed in a manner that supports a high degree of confidence that the control is complete, consistent, and correct.

What's in the game plan moving forward?

2010 and Beyond Focus Areas

- Common Security Standards and Guidance
- Developmental Security
  - Systems and Security Engineering
  - Application Security
- Operational Security
  - Security Content Automation Protocol Initiative and Future Extensions (network devices, mainframes)
  - Continuous Monitoring
- Education, Training, and Awareness
- Prototypes and Use Cases
  - Industrial Control Systems

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Leader

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Administrative Support

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

Senior Information Security Researchers and Technical Support

Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

Pat Toth
(301) 975-5140
patricia.toth@nist.gov

Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Matt Scholl
(301) 975-2941
matthew.scholl@nist.gov

Information and Feedback
Web: csrc.nist.gov/sec-cert
Comments: sec-cert@nist.gov